ARMY RESEARCH LABORATORY

Virtual User Interface for C^3 Net Battle Management

John Brand and John Nichols

ARL-MR-374 October 1998

Approved for public release; distribution unlimited.

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory

Adelphi, MD 20783-1197

ARL-MR-374 **October 1998**

Virtual User Interface for C^3 Net Battle Management

John Brand

Information Science and Technology Directorate, ARL

John Nichols

Quality Research, Inc.

Abstract

A virtual reality network management and analysis software package, inspired by a project reported initially by British Telecom, is being developed for the U.S. Army Research Laboratory (ARL) under a Small Business Innovative Research (SBIR) program with Quality Research, Inc. The Phase I feasibility demonstrator led to a Phase II development effort. The software package acts as a data management and display device, acquiring information on network status in a variety of ways, processing the network status information, and displaying it in a two-dimensional platform, superimposed on digitized three-dimensional map data, perspective view from a steerable viewpoint, or in three-dimensional color, real-time virtual reality, using display goggles. This will allow management of tactical and strategic battlefield communications networks in real time and facilitate pre-battle planning and post-battle or post-exercise analysis of network performance.

Contents

1. The Virtual User Interface **1**

2. The Threat to Combat Networks **2**

3. The VR Tool **4**

4. Phase I Results **7**

5. Use **8**

6. Summary **9**

References **9**

Distribution **11**

Report Documentation Page **13**

Figures

1. Program architecture 4
2. The display 6

1. The Virtual User Interface

The U.S. Army Research Laboratory (ARL) is conducting a Phase II Small Business Innovative Research (SBIR) program with Quality Research, Inc. (QRI), to develop a virtual reality (VR) software package for communications network management. The successful Phase I program resulted in a feasibility demonstrator called the Situation Awareness Virtual Environment for Networks (SAVENet). The follow-on Phase II project began in December 1997. The software package will provide a virtual user interface (VUI) that will enable network managers to "immerse" themselves in their network. Immersion is the psychological term for a process that should allow network managers to vastly enhance network status and situation awareness by sensing the network status in a global sense, in real time.* This situation awareness should provide both a fighting tool and a peacetime network management tool. The ability to present network events provided either by playback of real or simulated traffic or by use with an interactive network engineering model should open new opportunities in training. Another application of intense interest to network researchers is that the VUI should also improve the ability of an analyst to gain insight into what happens during simulations, experiments, and live exercises.

Immersion will be gained by using either a flat screen display of a three-dimensional (3-D) perspective of the network spread over the battle area, with simple status monitoring symbols, or by a true 3-D real-time color representation viewed by VR goggles. These network representations are superimposed, along with tactical overlays, on a 2-D or 3-D map or other digital representation of the environment. A separate effort is under way to provide statistical packages similar to those in commercial large-scale network engineering tools, such as OPNET. Status alarms can be set on selected net parameters to gain early warning of net intrusion or operation of malicious software such as a worm or virus attack. Other network management tools exist to perform similar functions for the office network environment and, typically, are large, single purpose, and expensive.

The concept is adapted from a display developed by British Telecom (BT) to monitor the British telephone network [1]. The idea of adapting the basic idea to management of a combat network, including the "tactical internet," was selected by ARL under the SBIR program in 1996.

*Immersion is discussed at some length in *The Design of Virtual Environments*, by Rory Stuart, McGraw Hill (1996), pp 65–67.

2. The Threat to Combat Networks

A combat net faces the synergistic threats of physical and "cyber" damage. The protection of Army combat nets, both tactical and logistic, occupies a corner of a phenomenon called defensive information warfare (DIW). A physically or cybernetically damaged net cannot tolerate as much degradation due to malicious programming (unauthorized access) or malicious programs (viruses, Trojan horses, etc) [2]. Survival of the combat network and the force it supports demands that network management compensate for both physical, or hard damage, and cyber, or soft damage, and that it adapt to changing battle conditions.

The cyber threat entities are amateur hackers; insiders; or dedicated professional hackers working alone, as members of supranational groups, or in the service of nation states. According to the Defense Science Board, the threat can be looked at as both structured and unstructured. In terms of a structured threat, there are over 100 nations with the capability to do damage, of which "more than 50 target the United States" [3]. Some have computer intelligence efforts. The unstructured threat involves 25 countries with computer underground groups, as well as very sophisticated individual hackers, many active on an international basis. Moreover, "a large structured attack with strategic intent against the United States could be prepared and exercised under the guise of unstructured activities" [3].

The effects can range from interruption of service to theft or corruption of information. Some of the tools of the computer criminal or hostile agent are malicious software such as worms or viruses. Viruses can be devastating to a network. Thus far, they have attracted the most media attention. Other kindred programs can be as destructive.*

There is a whole area on the World Wide Web (www) devoted to viruses and their kin, and a lively market in antivirus programs. The virus threat is growing and mutating constantly. Analysts at IBM have estimated that five new viruses a day are created [4]. Additionally, the Internet Worm of 1988 brought down portions of the Internet for some time, which created an indelible impression in the minds of users. It has not happened since then, but the potential frightens many [5].

According to Martin Libicki [6],

> *The Computer Emergency Response Team] CERT received over 2,000 reports [of break-ins] in 1994 (a rise apace with the Internet's growth—but CERT today is but one of over 20 incident centers, albeit the one everyone knows of). The Defense Information Systems Agency used publicly distributed tools to attack unclassified defense systems. It worked eight of nine times. Only 1 of 20 victims knew they were attacked, and only 1 in 20 of "them" reported it as they should have. If this 400:1 ratio is indicative—and Navy tests echo this—then 200 reports represent a million internet break-ins, even if very few do real damage.*

*A great deal of information is available on the World Wide Web at sites such as www.infowar.com.

Much of this is due to lack of security discipline. For instance, the "sendmail" bug, exploited to create the Internet Worm (1988), was used by hackers to break into computers in Rome Labs (1994) and Los Alamos (1996)—it had not been fixed at those sites even then [6]. Simple tools that are widely available also contribute to the danger: one can download a "war-dialer" from the Internet; access a target's web page, often with a telephone book with names, office symbols, fax numbers, e-mail addresses, etc; and go to work immediately. If the fax number is connected to certain types of fax modems on a PC, left on autoreceive, and the system administrator does not know the machine exists, illicit access can be gained. One speaker at a recent InfoWarCon reported that, in a survey of a company's security, the group spent a day trying to break in. At the end of the day, someone remembered a business card from a vice president that gave a fax number. Within minutes they were in.

Viruses:

- The first virus released in the wild was created by a Pakistani computer dealer [6].
- Two-thirds of the doctorates in computer science go to non-U.S. recipients, many from India, Pakistan, and Iran.
- One U.S. government organization examined all hardware and software that reached its loading dock and found "500 different computer viruses *in shrink-wrapped products coming directly from the factory*" [emphasis in original] [6].
- Anecdote—take it for what it is worth: a colleague in civil affairs/ PSYOPS mentioned that computers returned from deployments are so virus-infested as to be unusable.

Legislation designed to deter hackers and other computer vandals or criminals has been evolving in the United States, but not fast enough. In any case, military networks in an expeditionary force will not be protected against enemies by U.S. legislation. This network management tool has the potential for being a practical tool for DIW.

It is no secret that the United States is taking measures to gain a defensive capability in information warfare (IW). These measures are best described as antihacker, and are both civil and military. The U.S. Air Force has activated a squadron to wage defensive IW, supported by an IW Battle Lab, and there are numerous civil committees and working groups [7]. The United States and the other industrialized states are most vulnerable to damage by theft or corruption of information; the payoff for an enemy is high, and the investment required is tiny.

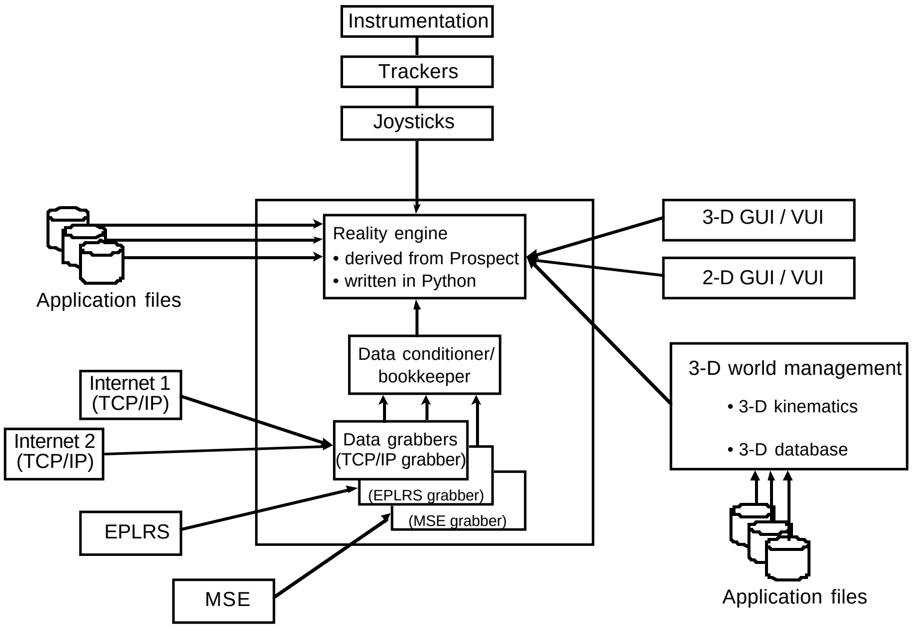
Additionally, the United States has now acknowledged an offensive IW operation [8].

3. The VR Tool

The Phase I effort was based on existing VR software and focused on a feasibility demonstration of a workable VUI. The demonstrator operated from a script of network events. The objective system to be pursued in Phase II will emphasize interaction with real networks and will begin to integrate existing ARL VR techniques to the maximum extent possible. The system will consist of a data grabber / bookkeeper, a data conditioner, a reality engine, and a display. The basic program architecture is shown in figure 1. The elements are listed below:

- *Data grabber/bookkeeper*. The tool is intended to function in several possible ways. Initially, the tool will use a script of the function of a representative tactical network. A tactical tool might use data from the GTE ISYSCON or use the network status information already generated by the Mobile Subscriber Equipment (MSE). In an additional effort, an interpretation module is being written to monitor a simulation using the distributed simulation protocols. Alternatively, in monitoring an internet, the machine can eavesdrop on the message traffic. In this way, it can keep track of who tries to talk to whom, whether they succeeded, when and how long the message was, who it was routed through, etc, and listen for the network management information generated under the Simple Network Management Protocol (SNMP). When any such data are captured, some status-reporting icon or subdisplay (BT calls them glyphs) will change accordingly. If the message loss rate or message delay becomes excessive, the bookkeeper can set the display to flag the fact for the network manager.
- *Data conditioner*. The data to be grabbed can consist not only of actual network management information, but also distributed interactive simulation (DIS) protocol data units (PDUs) or the successor protocol, the high

Figure 1. Program architecture.



level architecture (HLA), the datagrams shuttling across an internet, or even status parameters of an electrical power grid. The data from such disparate sources must be interpreted in a form usable for the bookkeeper, which then produces output for the reality engine.

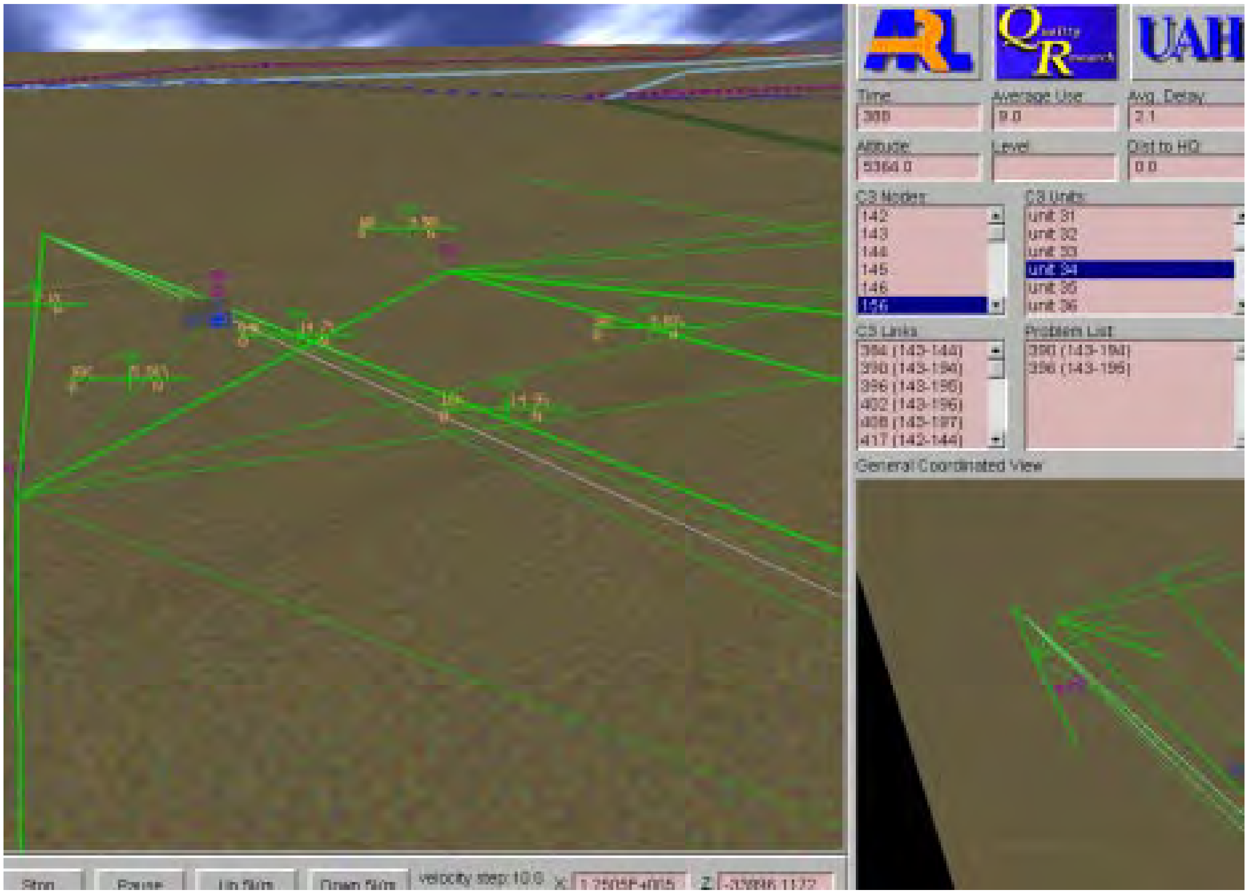
- *Reality engine*. The reality engine is based on commercial software that takes a description of the environment, be it the interior of a command post vehicle or National Imagery and Mapping Agency (NIMA) digital terrain and elevation data (DTED), and joins it with the data from the data conditioner. The reality engine is built on a software package called Prospect, which uses the Python simulation language.

- *Display*. The display can be either a 3-D perspective view of the net on a screen or a 3-D VR display. The point of view can be flown over the area covered by the net or the VR goggles can communicate where in the virtual space the net manager is looking, for the engine to synthesize the matching view. The display can lay the net flat on a map or superimpose the net on 3-D terrain generated from the digital data from the Defense Mapping Agency. Other options include superimposition of current aerial photography on the terrain. One display that appears very attractive is the ARL Virtual Sand Table. The Sand Table also uses the 3-D terrain plus tactical overlay data for tactical planning.

The Phase I demonstrator display is shown in figure 2. The resolution of the terrain shown is not photographic, nor need it be. For a signal person, high-fidelity representation of the more abstract terrain representation is adequate. A “drill-down” capability with better realism can be done to show site layout or even control board detail, for operator training.

The left box of the display is a perspective view of a portion of the battle area; location of the viewpoint and direction of view can be selected by the operator. The operator can fly the point of view manually, set an autopilot cruise, or transfer instantly to a given net element. Link and node status and identification are shown also. This view can be changed to a regular vertical map view if desired. The upper right box gives net statistical information and specific data on selected nodes and links and shows trouble areas, etc The lower right box is a navigation aid. It displays a segment of a map with the overlays as well as net elements and with the look direction and true north. This helps the operator remain oriented.

The Phase I program was compatible, through an interface program, with several platforms. This capability will be retained in Phase II. The platforms include a high-grade PC at the low end and workstations at the high end. The ability for essentially the same tool to run on a spectrum of machines simplifies the Army’s task of using the tool and makes the market much broader.



Time: 380

Average Use: 9.0

Avg. Delay: 2.1

Altitude: 5364.0

Level:

Dist to HQ: 0.0

C3 Nodes:
142
143
144
145
146
156

C3 Units:
unit 31
unit 32
unit 33
unit 34
unit 35
unit 36

C3 Links
384 (143-144)
390 (143-194)
396 (143-195)
402 (143-196)
408 (143-197)
417 (142-144)

Problem List
390 (143-194)
396 (143-195)

General Coordinated View

velocity step: 10.0 X: 1.2505E+005 Z: -33896.1172

Figure 2. The display.

4. Phase I Results

The Phase I effort produced a feasibility demonstration of the underlying tool and its VUI as it applies to the management of a battlefield communications network. The message traffic script, provided by GTE, was based on the simulated message traffic for a large force under combat conditions, produced by the GTE Multi Switch Simulation.

The current demonstrator runs on an Intergraph TDZ410, with two Pentium Pro 200 MHz processors and 128 megabytes of RAM. The machine has a Realism Graphics card with 128 Mbytes of Ram for texture. Prospect is written in C, with instructions in Open GL for 3-D graphics. Input files are in Python. The demonstrator uses an inexpensive 3-D headset made by Virtual I-O, which tracks head motion in yaw, pitch, and roll to allow computation of the view vector for the scene. 2-D displays, such as the screen display in figure 1, are on an ordinary monitor.

The scripted scenario can support a 6-minute or 21-minute scenario. The force is engaged near Kuwait City. Network management is illustrated for one division in this demonstration. There are 30 nodes and 27 links in this script. The equipment simulated is the MSE Packet Network (PN). The scripted actions include

- two examples of employment of radio relays to improve bit error rate (BER),
- two examples of forward error correction (FEC), and
- an illustration of the impact of traffic-loading on message speed of service.

5. Use

The software is intended to allow the manager of a combat network or a network administrator to manage a net using real-time information with a sense of global situation awareness. Net management tools exist that display various parameters on a flat screen and allow the operator to direct intense attention to a particular element. The VR element of this tool should allow the same intense scrutiny, with an out-of-the-corner-of-the-eye situation awareness that should allow a net manager to rapidly respond to problems while they are still small and local. The modularity of this program architecture also allows easy input of tactical overlays, other signals intelligence data, and other user-desired information. The whole battle becomes part of situation awareness as well as just circuits.

In the book *The Cuckoo's Egg*, an account is given of the invasion by and detection of the Internet Worm of 1988 [5]. One of the indicators of infection was the sudden avalanche of messages generated by an infected node. Another was the profound increase in machine capacity devoted to tasks related to Worm propagation; everything else ground to a halt. The net management tool can be made to display just that kind of information. If the net manager suspects an element is behaving atypically, he or she can excise the element, be it node or subnet. Likewise, a net damaged by artillery fire could be modified, perhaps, by changing access priority for certain units or adding additional gateways.

Internet failure due to congestion—congestion collapse—appears to have a fairly rapid onset [9]. There is also some indication that a combat net (not necessarily an internet) can be made to "lock up" when traffic exceeds a threshold. Lockup may be rapid once it begins, and messages from low-priority nodes are essentially eliminated, while other messages are slowed down tremendously. Under conditions of combat, when the message generation rate goes very high, the net may lose capacity from physical damage, jamming, and perhaps malicious programming. The loss of net capacity, plus a constant demand for attempted net traffic due to combat needs, means a corresponding increase in net load, which is the variable mentioned above in congestion failure. The net manager may be able to manage the net by limiting net access by some, changing access priorities, message "time-to-live," etc

Ultimately, the goal is to allow the combat net manager to "fly" a net like a fighter plane—or video game—with the same instant comprehension and reaction or allow an analyst to perceive factors with the same improvement to insight that real-time graphical output allowed when it became available.

6. Summary

ARL, in concert with QRI, is embarked on a quest for a software package that will give much-improved, real-time situation awareness and problem comprehension to a network manager. This will allow improved analysis, problem solving, planning, and training. It will also allow better management in the lab, on the field of battle, and in a host of civil networks, from small local area networks to larger cyber worlds.

References

1. Lowe, Robert, “Three UK Studies in Virtual Reality,” *Virtual Reality World* (March–April 1994), pp 51–54.
2. Hoffman, L. (ed.), *Rogue Programs: Viruses, Worms, and Trojan Horses*, Van Nostrand Reinhold (1990).
3. Office of the Under Secretary of Defense for Acquisition and Technology, *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield.* AD-A286 745, figure 4-2 (October 1994), p 24.
4. Nance, B., “Keep Networks Safe From Viruses,” *BYTE* (November 1996), pp 167–175.
5. Stoll, Clifford, *The Cuckoo’s Egg*, Doubleday, New York (1989); Pocket Books (1995).
6. Libicki, Martin, “Protecting the United States in Cyberspace,” *Cyberwar,* A. Campen, D. Dearth, and R. Gooden, eds., AFCEA International Press, Fairfax, VA (1996).
7. Kerr, J., “Information Assurance: Implications to National Security and Emergency Preparedness,” *Cyberwar*, A. Campen, D. Dearth, and R. Gooden, eds., AFCEA International Press, Fairfax, VA (1996), p. 257ff.
8. Brewin, B., and H. Harreld, “DOD Adds Attack Capability to Infowar,” Federal Computer Week (March 1998) , pp. 1, 2.
9. Comer, Douglas E., *Internetworking With TCPIIP*, **1**, Prentice Hall, Englewood Cliffs, NJ (1991), p. 192.

Distribution

Admnstr
Defns Techl Info Ctr
Attn DTIC-OCP
8725 John J Kingman Rd Ste 0944
FT Belvoir VA 22060-6218

Ofc of the Dir Rsrch and Engrg
Attn R Menz
Pentagon Rm 3E1089
Washington DC 20301-3080

Ofc of the Secy of Defns
Attn ODDRE (R&AT)
Attn ODDRE (R&AT) S Gontarek
The Pentagon
Washington DC 20301-3080

OSD
Attn OUSD(A&T)/ODDDR&E(R) R J Trew
Washington DC 20301-7100

AMCOM MRDEC
Attn AMSMI-RD W C McCorkle
Redstone Arsenal AL 35898-5240

CECOM
Attn PM GPS COL S Young
FT Monmouth NJ 07703

Dir for MANPRINT
Ofc of the Deputy Chief of Staff for Prsnnl
Attn J Hiller
The Pentagon Rm 2C733
Washington DC 20301-0300

Hdqtrs Dept of the Army
Attn DAMO-FDT D Schmidt
400 Army Pentagon Rm 3C514
Washington DC 20301-0460

US Army Edgewood RDEC
Attn SCBRD-TD J Vervier
Aberdeen Proving Ground MD 21010-5423

US Army Info Sys Engrg Cmnd
Attn ASQB-OTD F Jenia
FT Huachuca AZ 85613-5300

US Army Natick RDEC Acting Techl Dir
Attn SSCNC-T P Brandler
Natick MA 01760-5002

US Army Rsrch Ofc
4300 S Miami Blvd
Research Triangle Park NC 27709

US Army Simulation, Train, & Instrmntn
Cmnd
Attn J Stahl
12350 Research Parkway
Orlando FL 32826-3726

US Army Tank-Automtv & Armaments
Cmnd
Attn AMSTA-AR-TD M Fisette
Bldg 1
Picatinny Arsenal NJ 07806-5000

US Army Tank-Automtv Cmnd Rsrch, Dev,
& Engrg Ctr
Attn AMSTA-TA J Chapin
Warren MI 48397-5000

US Army Test & Eval Cmnd
Attn R G Pollard III
Aberdeen Proving Ground MD 21005-5055

US Army Train & Doctrine Cmnd
Battle Lab Integration & Techl Dirctrt
Attn ATCD-B J A Klevecz
FT Monroe VA 23651-5850

US Military Academy
Mathematical Sci Ctr for Excellence
Attn MDN-A MAJ M D Phillips
Dept of Mathematical Sci Thayer Hall
West Point NY 10996-1786

Nav Surface Warfare Ctr
Attn Code B07 J Pennella
17320 Dahlgren Rd Bldg 1470 Rm 1101
Dahlgren VA 22448-5100

DARPA
Attn B Kaspar
3701 N Fairfax Dr
Arlington VA 22203-1714

Univ of Texas at Austin
Inst for Advncd Tchnlgy
PO Box 202797
Austin TX 78720-2797

Distribution (cont'd)

University of Texas ARL Electromag Group
Attn Campus Mail Code F0250 A Tucker
Austin TX 78713-8029

Hicks & Associates, Inc
Attn G Singley III
1710 Goodrich Dr Ste 1300
McLean VA 22102

Quality Rsrch Inc
Attn J Nichols
150 West Park Loop Ste 302
Huntsville AL 35802

US Army Rsrch Lab
Attn AMSRL-CI-LP (305)
Aberdeen Proving Ground MD 21005

US Army Rsrch Lab
Attn AMSRL-IS-T J Brand (5 copies)
Aberdeen Proving Ground MD 21005-5067

US Army Rsrch Lab
Attn AMSRL-CI-LL Techl Lib (3 copies)
Attn AMSRL-CS-AL-TA Mail & Records
Mgmt
Attn AMSRL-CS-EA-TP Techl Pub (3 copies)
Attn AMSRL-D J Lyons
Attn AMSRL-DD J Rocchio
Adelphi MD 20783-1197

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** October 1998	**3. REPORT TYPE AND DATES COVERED** Final, June 1997 to June 1998

4. TITLE AND SUBTITLE Virtual User Interface for C^3 Net Battle Management

5. FUNDING NUMBERS

DA PR: AH48

PE: 6.1

6. AUTHOR(S) John Brand (ARL), John Nichols (Quality Research, Inc.)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Research Laboratory
Attn: AMSRL-IS-T
2800 Powder Mill Road
Adelphi, MD 20783-1197

email: jbrand@arl.mil

8. PERFORMING ORGANIZATION REPORT NUMBER

ARL-MR-374

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Research Laboratory
Aberdeen Proving Ground, MD 21005-5067

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

ARL PR: 8TEP10
AMS code: 611102H4811

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

A virtual reality network management and analysis software package, inspired by a project reported initially by British Telecom, is being developed for the U.S. Army Research Laboratory (ARL) under a Small Business Innovative Research (SBIR) program with Quality Research, Inc. The Phase I feasibility demonstrator led to a Phase II development effort. The software package acts as a data management and display device, acquiring information on network status in a variety of ways, processing the network status information, and displaying it in a two-dimensional platform, superimposed on digitized three-dimensional map data, perspective view from a steerable viewpoint, or in three-dimensional color, real-time virtual reality, using display goggles. This will allow management of tactical and strategic battlefield communications networks in real time and facilitate pre-battle planning and post-battle or post-exercise analysis of network performance.

14. SUBJECT TERMS

Virtual reality, network management, information warfare

15. NUMBER OF PAGES

19

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** SAR

DEPARTMENT OF THE ARMY
U.S. Army Research Laboratory
2800 Powder Mill Road
Adelphi, MD 20783-1197